

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

JACQ NIENABER, on behalf of herself
and all others similarly situated,

Plaintiff,

v.

OVERLAKE HOSPITAL MEDICAL
CENTER,

Defendant.

CASE NO. 2:23-cv-01159-TL

ORDER ON MOTION TO DISMISS
SECOND AMENDED CLASS
ACTION COMPLAINT

This matter is before the Court on Defendant Overlake Hospital Medical Center's Motion to Dismiss Plaintiff's Second Amended Class Action Complaint under Rule 12(b)(6) and Motion to Strike Certain Claims under Rule 12(f). Dkt. No. 54. Having considered Plaintiff Jacq Nienaber's opposition (Dkt. No. 55) and Defendant's reply (Dkt. No. 56), as well as Defendant's notice of supplemental authority (Dkt. No. 57), and finding oral argument unnecessary, *see* LCR 7(b)(4), the Court GRANTS IN PART and DENIES IN PART Defendant's motion.

I. BACKGROUND

A. Factual Background

The Court assumes familiarity with the facts of this case. Briefly, in Plaintiff’s Second Amended Class Action Complaint (“SAC”), Plaintiff, a current patient of Defendant, alleges that Defendant, a nonprofit healthcare organization, installed and implemented browser plugins—including the Facebook Tracking Pixel (“Pixel”), Facebook’s Conversions Application Programming Interface (“Conversions API”), and Google’s Tag Manager and Analytics tools—on its website <https://www.overlakehospital.org> (“the Website”), through which patients (and members of the public) can “conduct searches about various medical conditions and treatments and the practitioners at each location who provide medical services.” Dkt. No. 49 ¶¶ 2–3. The Website also allows patients to log in to Defendant’s private patient portal. *Id.* Plaintiff alleges that she has used the Website to, among other things, search for healthcare providers, pay bills, research and identify treatment options, and log into Defendant’s patient portal. *Id.* ¶¶ 46–47 (sealed).

Plaintiff alleges that Defendant uses the plugins in order to track and enable the transmission and disclosure of information from visitors to Defendant’s Website to third parties, including Facebook and Google. *Id.* ¶¶ 3–11, 68. The data transmitted includes Plaintiff’s and Class Members’ “health conditions; [] desired medical treatment or therapies; and [] phrases and search queries (such as searches for symptoms, treatment options, or types of providers.” *Id.* ¶ 104. Further, the Pixel additionally transmits website users’ Facebook IDs, “thereby allowing individual patients’ communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts and therefore their identity.” *Id.* ¶ 105. The Google Tag Manager tool transmits to Google any search phrases typed into the general search bar located on Defendant’s home page. *Id.* ¶ 117–18.

1 As Defendant's patient, Plaintiff "expected that her online communications with
2 Defendant were solely between herself and Defendant, such communications would not be
3 transmitted or intercepted by a third party," and Defendant would safeguard her private
4 information. *Id.* ¶ 52. She alleges that "[d]irectly after using Defendant's Website in relation to
5 her [medical issues], Plaintiff saw targeted advertisements on her Facebook and Instagram
6 accounts advertising [related treatment therapies and care]." *Id.* ¶ 57 (sealed).

7 Plaintiff contends that Defendant's transmissions of information violated its own privacy
8 policies, HIPAA standards, and industry standards. *Id.* ¶¶ 129–33 (privacy policies), 134–41
9 (HIPAA standards), 142–46 (industry standards). She reasserts claims for negligence, invasion of
10 privacy, breach of implied contract, unjust enrichment, violation of the Electronic
11 Communications Privacy Act, and violation of the Washington Consumer Protection Act. *See*
12 *generally* Dkt. No. 49. Plaintiff also newly brings claims for breach of fiduciary duty and
13 violation of RCW §§ 7.70.010–.160. *See generally id.*

14 **B. Procedural Background**

15 On May 13, 2024, the Court granted Defendant's Rule 12(b)(6) motion to dismiss
16 Plaintiff's original complaint with leave to amend. Dkt. No. 32. The Court found in part that
17 Plaintiff had failed to make specific allegations as to "what information she gave to Defendant,
18 and what information Defendant in turn shared with third parties," as well as allegations that
19 "Defendant shared information that can be used to readily identify her." *Id.* at 15. Plaintiff filed
20 an amended class action complaint on June 21, 2024. Dkt. No. 35 (sealed). Following the
21 Parties' stipulation (Dkt. Nos. 45 (stipulation), 46 (order)), Plaintiff filed her SAC on August 2,
22 2024 (Dkt. No. 49 (sealed)).

23 Plaintiff's SAC includes additional allegations regarding the specific information she
24 shared with Defendant, as well as the information she contends was shared with third parties.

Dkt. No. 49 ¶¶ 46–48 (sealed); *see also id.* ¶ 57 (sealed). Plaintiff also added a number of allegations regarding the inherent value of her private information and the value gained by Defendant by sharing her information. *Id.* ¶¶ 122–28.

Defendant now moves to dismiss Plaintiff’s SAC under Rule 12(b)(6) and to strike certain claims under Rule 12(f). Dkt. No. 54.

II. LEGAL STANDARD

A. Motion to Strike

A court “may strike from a pleading an insufficient defense or any redundant, immaterial, impertinent, or scandalous matter.” Fed. R. Civ. P. 12(f). In deciding a Rule 12(f) motion to strike, a court should not resolve disputed and substantial factual or legal issues. *See Whittlestone, Inc. v. Handi-Craft Co.*, 618 F.3d 970, 973–75 (9th Cir. 2010) (“We . . . hold that Rule 12(f) does not authorize district courts to strike claims for damages on the ground that such claims are precluded as a matter of law.”). “The function of a [Rule] 12(f) motion to strike is to avoid the expenditure of time and money that must arise from litigating spurious issues by dispensing with those issues prior to trial” *Id.* at 973 (quoting *Fantasy, Inc. v. Fogerty*, 984 F.2d 1524, 1527 (9th Cir. 1993), *rev’d on other grounds*, 510 U.S. 517 (1994)). Rule 12(f) motions to strike are generally disfavored because the motions may be used as delay tactics and because of the strong policy favoring resolution on the merits. *E.g., Chao Chen v. Geo Grp., Inc.*, 297 F. Supp. 3d 1130, 1132 (W.D. Wash. 2018) (citations and internal quotation marks omitted).

B. Motion to Dismiss

A complaint must include “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2).

A defendant may seek dismissal when a plaintiff fails to state a claim upon which relief can be granted. Fed. R. Civ. P. 12(b)(6). In reviewing a Rule 12(b)(6) motion to dismiss, the

1 Court takes all well-pleaded factual allegations as true and considers whether the complaint
 2 “state[s] a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678
 3 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). While “[t]hreadbare
 4 recitals of the elements of a cause of action, supported by mere conclusory statements,” are
 5 insufficient, a claim has “facial plausibility” when the party seeking relief “pleads factual content
 6 that allows the court to draw the reasonable inference that the defendant is liable for the
 7 misconduct alleged.” *Iqbal*, 556 U.S. at 672. When reviewing a dismissal pursuant
 8 to Rule 12(b)(6), “we accept as true all facts alleged in the complaint and construe them in the
 9 light most favorable to plaintiff[], the non-moving party.” *DaVinci Aircraft, Inc. v. United*
 10 *States*, 926 F.3d 1117, 1122 (9th Cir. 2019) (alteration in original) (quoting *Snyder & Assocs.*
 11 *Acquisitions LLC v. United States*, 859 F.3d 1152, 1156–57 (9th Cir. 2017)).

12 III. DISCUSSION

13 A. Motion to Strike

14 1. Exhibit A to Plaintiff’s Opposition

15 Plaintiff’s Exhibit A is a series of charts listing and briefly summarizing caselaw from
 16 various federal courts that Plaintiff considers to be relevant to its opposition. *See generally* Dkt.
 17 No. 55-1. These charts are grouped under largely unargumentative headings, such as “Online
 18 Tracking Technology Orders Denying Motions to Dismiss” (Dkt. No. 55-1 at 2) and “Online
 19 Tracking Technology Motion to Dismiss Orders Allowing Negligence Claims” (*id.* at 19). As
 20 Defendant points out, the charts do not include “discussion of the specific facts at issue in [the]
 21 cases or the courts’ analyses.” Dkt. No. 56 at 7. Defendant argues in its reply that the Court
 22 should strike Exhibit A, which is attached to Plaintiff’s opposition. Dkt. No. 56 at 7. Defendant
 23 argues that Exhibit A circumvents the page limit proscribed by LCR 7(e)(3) by “purporting to
 24 characterize various motions to dismiss that were denied in purportedly ‘similar’ cases . . . ,

1 noting that certain causes of action survived such motions—without any discussion of the
2 specific facts at issue in those cases or the courts’ analyses in reaching those decisions.” *Id.*
3 (internal citation omitted).

4 On the one hand, the Court certainly understands Defendant’s concern. On the other
5 hand, a court may allow the use of non-argumentative summary exhibits containing relevant
6 citations where they do not engage in argument or one-sided analysis. *See Persad v. Ford Motor*
7 *Co.*, No. C17-12599, 2019 WL 3936368, at *2 (E.D. Mich. Aug. 20, 2019). Such a chart *could*
8 be a useful reference tool for a court in certain situations. However, the Court finds Plaintiff’s
9 charts unhelpful here as the critical analysis on a motion to dismiss is the sufficiency of the facts
10 pleaded in a complaint. Without knowing the facts that were pleaded in the cases cited in
11 Plaintiff’s exhibit, the Court simply cannot draw any conclusions about the applicability of the
12 rationale or decisions of those cases to the one at hand. If there were any cases that would have
13 been particularly probative, Plaintiff should have included them in the body of her brief or made
14 a timely request for an over-length brief if additional space was needed.

15 Accordingly, Exhibit A is STRICKEN.

16 **2. Plaintiff’s Fifth and Sixth Claims**

17 Plaintiff added two new claims to her SAC: a fifth claim for breach of fiduciary duty and
18 a sixth claim for violation of RCW §§ 7.70.010–.160. *Compare* Dkt. No. 35 (first amended
19 complaint), *with* Dkt. No. 49 (second amended complaint). Defendant moves to strike these two
20 new claims because they exceed the scope of the Court’s prior Order. Dkt. No. 54 at 21.
21 Defendant argues that the Court granted Plaintiff leave to amend certain specific causes of
22 action, and that Plaintiff did not obtain Defendant’s consent or leave from the Court to add the
23 two new claims. *Id.*

1 The Court's first dismissal order did not contain any limitation with respect to
 2 amendments Plaintiff might make. *See* Dkt. No. 32 at 34. Following the filing of Plaintiff's first
 3 amended complaint, the Parties "met and conferred regarding anticipated Motion to Dismiss
 4 Plaintiff's Amended Complaint *and agreed to allow Plaintiff to file a Second Amended*
 5 *Complaint.*" Dkt. No. 45 at 2 (emphasis added). The Parties did not include any limitation on
 6 Plaintiff's ability to file a second amended complaint. *See id.* The Court granted the Parties'
 7 stipulation (Dkt. No. 46), and Plaintiff subsequently filed the SAC.

8 Because the Court did not place any limitations on the leave granted to Plaintiff to amend
 9 her complaint, Defendant consented to the filing of the SAC, and this case is in the early stages
 10 (and therefore, Plaintiff would have been granted leave to add the claims pursuant to Federal
 11 Rule of Civil Procedure 15(a)(2) if she had filed such a motion), the Court declines to strike
 12 Plaintiff's two new causes of action.

13 Accordingly, Defendant's motion to strike Plaintiff's fifth and sixth claims is DENIED.

14 **B. Motion to Dismiss**

15 **1. Whether the SAC Alleges the Disclosure of Personally Identifiable** 16 **Information or Protected Health Information**

17 This case concerns the misuse and transfer of confidential personally identifiable
 18 information ("PII") and protected health information ("PHI") (collectively referred to as "Private
 19 Information").¹ The principal theory of Plaintiff's case, which underlies all claims, is that
 20 Defendant transmits to third parties the Private Information that patients input into Defendant's
 21
 22
 23

24 ¹ Confidential and individually identifiable health information, referred to in the SAC as PHI, is also commonly referred to as Individually Identifiable Health Information ("IIHI").

public website,² without those patients’ consent. Dkt. No. 49 ¶¶ 2, 25, 46 (sealed). As the Court discussed in its prior Order:

[T]he transmission of information submitted to a *private patient portal*—such as a user clicking on the “log in” button on that webpage—reveals patient status, which in and of itself is protected health information. *See, e.g., In re Meta Pixel Healthcare Litig. (In re Meta Pixel I)*, 647 F. Supp. 3d 778, 791–93 (N.D. Cal. 2022); *Cousin v. Sharp Healthcare (Cousin I)*, 681 F. Supp. 3d 1117, 1123–24 (S.D. Cal. 2023). The collection and transmission of information from unauthenticated web pages (*i.e.*, pages that do not require a user to log in to access the website) may be actionable as well if the information disclosed demonstrates that the plaintiff’s interactions plausibly relate to the provision of healthcare, or if the information connects a particular user to a particular healthcare provider (*i.e.*, patient status). *See Cousin v. Sharp Healthcare (Cousin II)*, 702 F. Supp. 3d 967, 973 (S.D. Cal. 2023); *In re Meta Pixel I*, 647 F. Supp. 3d at 793; *In re Meta Healthcare Pixel Litig. (In re Meta Pixel II)*, 713 F. Supp. 3d 650, 654–55 (N.D. Cal. 2024). However, where nothing but browsing activity on a publicly available website is transmitted, courts within this circuit have held that “the URLs, or the content of the pages located at those URLs, [do not relate] ‘to the past, present, or future physical or mental health or condition of an individual.’” *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 955 (N.D. Cal. 2017) (quoting 45 C.F.R. § 160.103), *aff’d*, 745 F. App’x 8 (9th Cir. 2018); *see also Cousin I*, 681 F. Supp. 3d at 1123.

Dkt. No. 32 at 6.

Plaintiff argues that the SAC alleges more than just “[t]racking’ of a ‘[p]ublic’ [w]ebsite” because Defendant’s website “is used by *patients* as part of their continuum of medical care,” relying primarily on *Doe v. Bon Secours Mercy Health*, No. A2002633, 2021 WL 9939010 (Ohio Com. Pl. Nov. 22, 2021), to support this distinction. Dkt. No. 55 at 9 (emphasis in original). But as the Court previously determined, the transmission of information from an

² The “Website” is defined in the SAC as Defendant’s public website, www.overlakehospital.org, where “patients can conduct searches about various medical conditions and treatments and the practitioners at each location who provide medical services,” as well as “pay bills, search for providers with whom to book appointments, and log in to Overlake’s MyChart Patient Portal.” Dkt. No. 49 ¶ 2.

1 unauthenticated website—even if the user is a patient—is only actionable where the information
2 disclosed either (1) “demonstrates that the plaintiff’s interactions plausibly relate to the provision
3 of healthcare,” or (2) “connects a particular user to a particular healthcare provider” or otherwise
4 identifies patient status, which is protected health information. Dkt. No. 32 at 6 (citing *Cousin II*,
5 702 F. Supp. 3d at 973); *see also Bon Secours*, 2021 WL 9939010, at *2 (“Plaintiff alleges that
6 the information disclosed to third parties *includes the fact that a visitor to defendant’s website is*
7 *a patient of defendant.*” (emphasis added)). That Plaintiff is a patient of Defendant does not
8 automatically mean that her browsing activity on Defendant’s public website is protected health
9 information.

10 But in the SAC, Plaintiff alleges that she used Defendant’s website to research specific
11 medical conditions and symptoms, identify treatment options, pay bills, research particular
12 doctors and specialists, and log in to Defendant’s private patient portal, and that Defendant
13 disclosed that information to third parties via the use of APIs and Pixels integrated on
14 Defendant’s website. Dkt. No. 49 ¶ 46 (sealed); *see also id.* ¶¶ 12–23, 47–48 (sealed). These
15 interactions with Defendant’s website plausibly relate to the provision of healthcare and,
16 importantly, disclose Plaintiff’s patient status, and the allegedly transmitted information in
17 Plaintiff’s SAC is comparable to information that other courts have found to be protected.

18 For example, in *Cousin II*, allegations that a plaintiff had used a public hospital website
19 to “search for a primary care physician” and had “filtered the results of Sharp [Memorial
20 Hospital]’s physician directory by, among other things, specialty,” narrowly survived dismissal
21 “by demonstrating that [plaintiff’s] interactions plausibly relate[d] to the provision of health
22 care.” 702 F. Supp. 3d at 973. Where additional *Cousin II* plaintiffs had “set forth their particular
23 medical conditions” and alleged that they “searched Defendant’s website for doctors who
24 specialize in these conditions and for information about their conditions (*i.e.*, symptoms,

1 treatments, procedures),” the *Cousin II* court again found that this information was protected
2 because the “interactions plausibly convey information about a present medical condition and the
3 provision of medical care covered by HIPAA.” *Id.*; see also, e.g., *In re Meta Pixel II*, 713 F.
4 Supp. 3d at 653–55 (finding sufficient allegations of disclosure of private information where
5 defendant disclosed “the health conditions for which they sought treatment or services, as well as
6 examples of their queries, appointment requests, or other information and services about which
7 they communicated with their providers”); *Kurowski v. Rush Sys. for Health*, No. C22-5380,
8 2023 WL 8544084, at *3 (N.D. Ill. Dec. 11, 2023) (finding that plaintiff had alleged disclosure
9 of personal health information where defendant transmitted the “name and location of her
10 personal physician, as well as her physician’s specialty”).

11 Plaintiff here makes similar allegations. She sets forth her specific medical condition,
12 alleges that she researched that condition and its symptoms on Defendant’s website and used
13 Defendant’s website to research particular doctors and specialists, and alleges that she used the
14 website to log in to Defendant’s patient portal. Dkt. No. 49 ¶ 46 (sealed). Plaintiff asserts that
15 “[t]he specific information Facebook and Google received revealed her specific medical
16 symptoms and conditions and the fact that she was seeking and received medical treatment from
17 Defendant.” *Id.* ¶ 48 (sealed). Like the allegations in *Cousin II*, these allegations just barely
18 demonstrate that Plaintiff’s interactions with Defendant’s website plausibly relate to the
19 provision of health care; thus, these interactions constitute protected information, and the
20 transmission of such information may be actionable.

21 Defendant urges the Court to follow the reasoning of *American Hospital Association v.*
22 *Becerra* (“AHA”), 738 F. Supp. 3d 780 (N.D. Tex. 2024), to find that the types of disclosures
23 alleged in Plaintiff’s SAC are not Private Information protected by HIPAA. See Dkt. No. 54 at
24 12–13. AHA addressed the objections of hospital associations and a healthcare system to a

1 guidance document promulgated by the United States Department of Health and Human Services
2 that addressed “online tracking technology [that] connects the IP address of a user’s device (or
3 other identifying information) with a visit to a webpage addressing specific health conditions or
4 listing health care providers” and declares that that these items, when combined (referred to as
5 the “Proscribed Combination”), are “a sufficient combination of information to constitute IIHI if
6 the visit to the webpage is related to the individual's own health.” 738 F. Supp. 3d at 792; *see*
7 *also J.C. v. Catholic Health Sys. Inc.*, No. C23-796, 2024 WL 5136236, at *14 (W.D.N.Y. Aug.
8 29, 2024). The *AHA* court found that “because the individual does not also transmit their
9 subjective intent in using or searching for a webpage to the healthcare entity that owns the
10 webpage, the Proscribed Combination is not IIHI”:

11 Put simply, that information cannot become IIHI based solely on
12 the visitors’ subjective motive for visiting the page, which is not
13 information that the Revised Bulletin requires the healthcare
14 provider or third-party vendor to receive at all. . . . Thus, even after
15 multiple speculations, the Proscribed Combination could never fit
HIPAA’s definition of IIHI. . . . The above conclusion is far from
novel. Indeed, covered entities have long been allowed to disclose
PHI that does not identify the particular individual.

16 *J.C.*, 2024 WL 5136236, at *14; *AHA*, 738 F. Supp. 3d at 803–04.

17 But as the *J.C.* court noted in its analysis of the *AHA* decision, the *AHA* court did not
18 address allegations involving disclosure of “potential [individually identifiable health
19 information] along with an individual’s Facebook ID, which very specifically identifies an actual
20 individual”; instead, the *AHA* court addressed allegations involving the disclosure of only an IP
21 address, which identifies a specific device. *J.C.*, 2024 WL 5136236, at *14; *see also AHA*, 738 F.
22 Supp. 3d at 789 (“The Original Bulletin provided several hypotheticals that trigger HIPAA
23 obligations, including circumstances where an online technology connects (1) an individual’s IP
24 address with (2) a visit to a UPW addressing specific health conditions or healthcare

1 providers.”). Contrary to Defendant’s assertion (Dkt. No. 56 at 8), Plaintiff alleges that more
2 than “only an IP address” was disclosed to third parties. She also alleges the disclosure of her
3 Facebook ID, which “links the user to his/her Facebook profile” (Dkt. No. 49 ¶ 4). Because
4 Plaintiff alleges the disclosure of her specific identity through her Facebook ID, the *AHA* court’s
5 reasoning is unpersuasive here.

6 Importantly, Plaintiff also alleges that the information disclosed by Defendant includes
7 the fact that Plaintiff sought and received medical treatment from Defendant. Dkt. No. 49 ¶ 48.
8 The fact that Plaintiff sought and received medical treatment from Defendant is an identification
9 of her status as a patient of Defendant, making this information protected despite originating
10 from Defendant’s public website. *See Cousin II*, 702 F. Supp. 3d at 973. Further, this information
11 distinguishes Plaintiff’s browsing activity from the activity in *AHA*: because Plaintiff’s patient
12 status was part of the information allegedly disclosed by Defendant, a third party in receipt of
13 Plaintiff’s information could conceivably relate Plaintiff’s browsing activity on Defendant’s
14 website to the provision of healthcare by Defendant. Compared to the allegations in *AHA*, where
15 the court found that the plaintiff’s subjective intent in visiting defendant’s website was not
16 disclosed, the additional disclosure of Plaintiff’s patient status with Defendant makes her other
17 interactions with Defendant’s website, such as searching for particular physicians or researching
18 specific medical conditions, clearly related to the provision of healthcare by Defendant to
19 Plaintiff.

20 Because Plaintiff has alleged the transmission of protected information, the Court turns to
21 an evaluation of each of Plaintiff’s claims.

1 **2. Count I: Negligence**

2 Plaintiff brings an amended claim for negligence on behalf of herself and the putative
3 nationwide class. Dkt. No. 49 at 35. Defendant seeks dismissal, arguing that Plaintiff “still fails
4 to establish breach and cognizable damages.” Dkt. No. 54 at 13.

5 Under Washington law, negligence requires “(1) the existence of a duty to the plaintiff,
6 (2) a breach of that duty, (3) a resulting injury, and (4) the breach as the proximate cause of that
7 injury.” *Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d 1140, 1156 (W.D. Wash.
8 2017) (citing *Degal v. Majestic Mobile Manor*, 129 Wn.2d 43, 914 P.2d 728, 731 (1996)).

9 The Court previously held that Plaintiff adequately alleged that Defendant owed a duty to
10 keep health care information confidential under the Health Care Information Act (“HCIA”), to
11 keep PHI confidential under its own privacy policy, and to keep PII confidential under a theory
12 of misfeasance. Dkt. No. 32 at 13–15. The Court adopts the reasoning from its prior Order and
13 will not repeat it here.

14 However, relevant to this Order, the Court did previously find that Plaintiff’s original
15 complaint did not allege facts sufficient to establish the breach of that duty, as Plaintiff did not
16 make “specific allegations as to what information she gave to Defendant, and what information
17 Defendant in turn shared with third parties,” as well as allegations that “Defendant shared
18 information that can be used to readily identify her.” *Id.* at 15. But as discussed above, *see supra*
19 Section III.B.1., Plaintiff has now pleaded sufficient facts to allege that Defendant failed to
20 safeguard—and indeed, affirmatively shared—her PHI and PII. Plaintiff has also alleged that
21 Defendant shared³ information that can be used to readily identify her. *See* Dkt. No. 49 ¶¶ 105–
22

23 ³ It is unclear whether the Pixel that Defendant installed on its Website is the mechanism by which Plaintiff’s
24 Facebook ID was transmitted, or whether that information was transmitted by a cookie originating from Facebook.
See Dkt. No. 49 ¶ 105 n.20. However, interpreting Plaintiff’s allegations in the light most favorable to Plaintiff, the

06. Defendant argues that Plaintiff’s allegations regarding the timing of her disclosures to Defendant and the purportedly relevant advertisements on Facebook and Instagram are too conclusory and speculative to establish breach. Dkt. No. 54 at 14. However, these allegations support the reasonable inference that Defendant shared Plaintiff’s Private Information in the 2019 to 2020 time frame in order to target Plaintiff and other patients with advertisements for medical treatments. Dkt. No. 9 ¶¶ 45–46, 57–58. While the specific allegations Defendant points to would not, alone, suffice to allege a breach by Defendant, the allegations taken as a whole support the reasonable inference that Defendant breached its duty of care by affirmatively sharing Plaintiff’s information. Thus, Plaintiff has sufficiently alleged that Defendant breached its duty to keep her PHI and PII confidential under the HCIA, its own privacy policy, and a theory of misfeasance.

The Court previously noted that Plaintiff’s allegations regarding a resulting injury were insufficient, observing that injury or damages may be adequately alleged where a plaintiff alleges “a heightened risk of future identity theft, loss of privacy with respect to highly sensitive information, loss of time, and risk of embarrassment,” but that Plaintiff had not alleged any such facts. Dkt. No. 32 at 16 (quoting *Flores-Mendez v. Zoosk, Inc.*, No. C20-4929, 2021 WL 308543, at *3–4 (N.D. Cal. Jan. 30, 2021)). Plaintiff contends that she “has now substantially alleged a loss of privacy with respect to highly sensitive information.” Dkt. No. 55 at 12 (citing Dkt. No. 49 ¶¶ 39, 43–60 (sealed), 191, 203). She alleges that her injuries include: “(i) invasion of privacy; . . . [and] (iii) diminution and/or loss of value of the Private Information” Dkt. No. 49 ¶ 39. Defendant argues that in order to recover damages under a negligence theory, Plaintiff must plead facts “showing that she lost the opportunity to sell her information or that the value of

Court will at this time construe Plaintiff’s allegations as contending that Defendant caused the transmittal of Plaintiff’s Facebook ID, along with her Private Information, to third parties.

1 her information was somehow diminished” or that there is a reasonable probability that she will
2 suffer actual harm. Dkt. No. 56 at 9.

3 “Under Washington law, “[a]ctual loss or damage is an essential element in the
4 formulation of the traditional elements necessary for a cause of action in negligence The
5 mere danger of future harm, unaccompanied by present damage, will not support a negligence
6 action.” *Leonard v. McMenamins, Inc.*, No. C22-94, 2024 WL 4188974, at *6 (W.D. Wash. Sept.
7 13, 2024) (alterations in original) (quoting *Krottner v. Starbucks Corp.*, 406 F. App’x 129, 131
8 (9th Cir. 2010)). Plaintiff argues that her negligence claim should be permitted to go forward
9 where her alleged damages are solely loss of privacy with respect to highly sensitive
10 information. Dkt. No. 55 at 12. However, she cites no support for the proposition that loss of
11 privacy alone can constitute damages for a negligence claim under Washington law. Other courts
12 have dismissed claims for negligence under Washington law in the data-privacy context where
13 plaintiffs have not alleged that they “suffered direct financial losses because of the Breach . . . [or
14 that] their identity has been stolen.” *Leonard*, 2024 WL 4188974, at *6; *cf. Krefting v. Kaye-*
15 *Smith Enters. Inc.*, No. C23-220, 2023 WL 4846850, at *5 (W.D. Wash. July 28, 2023) (finding
16 damages for purposes of negligence claim under Washington law in data-privacy case where
17 plaintiff alleged fraudulent opening of a credit account and fraudulent credit inquiry using his
18 personal information). Plaintiff has not alleged any such misuse of her Personal Information.

19 At least one Washington court has recognized that the Washington Supreme Court has
20 not yet weighed in on the murky issue of whether the loss of value of PII is a type of harm that is
21 recoverable in negligence, but that courts addressing this issue have reached varying results.
22 *Nunley v. Chelan-Douglas Health Dist.*, 32 Wn. App. 2d 700, 721–23, 558 P.3d 513 (2024)
23 (analyzing cases). In reaching its ultimate conclusion, the *Nunley* court “note[d] that the laws in
24 Washington demonstrate a public policy that recognizes there is value in the security of our

1 personal information.” *Id.* at 723–24. “Considering Washington’s existing law and the realities
2 of the digital economy we live in now,” the *Nunley* court held that “a person’s means of
3 identification, PII and PHI, can have value and conceivably that value can be diminished or
4 destroyed when their identities are misappropriated for illegal purposes.”⁴ *Id.* at 724. Therefore,
5 “[t]he loss in value of . . . PII and PHI is a current harm and a cognizable injury sufficient to
6 support a cause of action for negligence.” *Id.* at 724–25. This Court agrees with the rationale of
7 the *Nunley* court.

8 In *Nunley*, one of the consequences of the loss of PII was that plaintiffs received
9 additional spam calls. *Id.* at 725. Similarly here, Plaintiff here alleges a loss of value of her
10 Private Information and that she received unsolicited advertisements related to her medical
11 condition following the disclosure of her information. But the *Nunley* plaintiffs also alleged that
12 at least one plaintiff’s Social Security number was found on the dark web and an unauthorized
13 business license had been opened in her name—comparable harms to other cases where
14 Washington courts found present damages as a result of a data breach. *Nunley*, 32 Wn. App. at
15 725; *see also Leonard*, 2024 WL 4188974, at *6; *Krefting*, 2023 WL 4846850, at *3. And the
16 Court has already determined that Plaintiff has not alleged any similar harm here.

17 Other courts have held that for plaintiffs to allege a diminution in value of their Private
18 Information, they must allege “(1) the existence of a market for [their Private Information], and
19 (2) an impairment of Plaintiff[’s] ability to participate in that market.” *Leonard*, 2024 WL
20 4188974, at *8 (citing *Griffey v. Magellan Health Inc.*, 562 F. Supp. 3d 34, 46 (D. Ariz. 2021)).
21 While Plaintiff makes no argument as to this theory of damages, she includes factual allegations
22

23 ⁴ Defendant’s supplemental authority (Dkt. No. 57) is inapt, as it analyzes this issue under Georgia law and focuses
24 on situations where PII had fallen into “a criminal’s hands.” Dkt. No. 57-1 (citation omitted). But the Court does not
read Washington law to be so limited as to require criminal activity.

1 detailing the value of her Personal Information (including her protected health information) to
 2 the best of her ability at this stage in the case,⁵ as well as allegations regarding the existence of a
 3 market for her private information. Dkt. No. 49 ¶¶ 122–28. But Plaintiff provides no information
 4 as to the second element: the impairment of her ability to participate in the market for her
 5 Personal Information. *Id.* ¶ 126. And “where ‘the crux of this case concerns [a third party’s
 6 receipt of [PII] that plaintiff[] apparently do[es] not want anyone other than [her] health care
 7 provider to have,’ it is incongruous for plaintiff ‘to then allege [she] intended to participate in
 8 this market. Or otherwise to derive economic value from [her] PII.’” *C.M. v. MarinHealth Med.*
 9 *Grp., Inc.*, No. C23-4179, 2024 WL 217841, at *2 (N.D. Cal. Jan. 19, 2024) (citation omitted).

10 Plaintiff’s SAC still does not clear the bar for her negligence claim, as she does not
 11 establish injury or damages. The Court is skeptical that Plaintiff will be able to establish her
 12 intent to participate in the market for her private information. However, Plaintiff nonetheless
 13 may be able to amend her complaint to sufficiently allege damages such as lost time and/or
 14 expenses in responding to the plausibly alleged misuse of her medical information and any other
 15 allegations that she believes supports the required showing of injury to support her negligence
 16 claim. *See id.* at *3. Therefore, the Court will permit one final amendment of Plaintiff’s claim for
 17 negligence.

18 Accordingly, as to Plaintiff’s claim for negligence, Defendant’s motion is GRANTED with
 19 leave to amend.

20 **3. Count II: Invasion of Privacy**

21 Plaintiff brings an amended claim for invasion of privacy on behalf of herself and the
 22 putative nationwide class. Dkt. No. 49 at 37. Defendant seeks dismissal, arguing that the SAC

23
 24 ⁵ Plaintiff notes that she cannot provide an actual valuation without discovery as Defendant holds exclusive control over the data that was disclosed as well as the return it received on its marketing investment. Dkt. No. 49 ¶ 126.

1 “does not cure the deficiencies the Court previously identified in the original complaint.” Dkt.
2 No. 54 at 14.

3 “Washington common law recognizes a ‘protectable interest in privacy [that] is generally
4 held to involve four distinct types of invasion: intrusion, disclosure, false light and
5 appropriation.’” *Buckley v. Santander Consumer USA, Inc.*, No. C17-5813, 2018 WL 1532671,
6 at *7 (W.D. Wash. Mar. 29, 2018) (quoting *Eastwood v. Cascade Broad. Co.*, 106 Wn.2d 466,
7 469, 722 P.2d 1295 (1986)); *see also Armijo v. Yakima*, No. C11-3114, 2012 WL 2576624, at *2
8 (E.D. Wash. July 3, 2012). Plaintiff argues that her invasion-of-privacy claim should survive
9 under a theory of intrusion upon seclusion. Dkt. No. 55 at 12–13.

10 “To prevail on an intrusion on seclusion claim, a plaintiff must prove that the defendant
11 (1) deliberately intruded; (2) into the plaintiff’s solitude, seclusion, or private affairs; (3) in a
12 manner that would be highly offensive to a reasonable person.” Dkt. No. 32 at 16 (quoting
13 *Armijo*, 2012 WL 2576624, at *2 (citing *Fisher v. State ex rel. Dep’t of Health*, 125 Wn. App.
14 869, 106 P.3d 836 (2005))). The Court previously determined that Plaintiff had not alleged a
15 deliberate intrusion by Defendant because Plaintiff voluntarily shared her information with
16 Defendant. Dkt. No. 32 at 18; *see also Buckley*, 2018 WL 1532671, at *7. But Plaintiff contends
17 that “Defendant has intruded into the seclusion of Plaintiff’s web browser, commandeering it to
18 transmit information to third parties to whom she never intended to transmit those details.” Dkt.
19 No. 55 at 13.

20 In support of her argument, Plaintiff cites to *In re Group Health Plan Litigation*, 709 F.
21 Supp. 3d 707 (D. Minn. 2023), where the court determined that plaintiffs’ claim that
22 “HealthPartners deliberately integrated Facebook Pixel and CAPI into its Website and servers,
23 which intercepted and shared communications with third parties” was “suggestive of intentional
24 intrusion” and was sufficient to state a claim at the motion-to-dismiss stage. 709 F. Supp. 3d at

714. But other courts have held the opposite. As the Court acknowledged in its Order on Defendant’s first motion to dismiss, the court in *Kurowski v. Rush System for Health*, 659 F. Supp. 3d 931 (N.D. Ill. 2023), held that “the harm for which Rush is responsible, if any, is its disclosure of patient data . . . not the obtaining of that data. The actual intrusion upon patients’ seclusion, via interception of their communications, is carried out by third parties.” 659 F. Supp. 3d at 944. Without binding precedent to consider, the Court declines to depart from the analysis in its prior Order, which determined that a claim for invasion of privacy could not be maintained under the facts alleged. *See* Dkt. No. 32 at 16–18.

Plaintiff additionally argues that “the Court should consider the relationship between the Plaintiff and her medical providers as one of seclusion, one where the two are alone properly privy to the information because a patient who cannot share their information with their doctor cannot receive medical services, often services essential to life and health.” Dkt. No. 55 at 13. While Plaintiff has not alleged the transmission of information from a private patient portal (*see* Dkt. No. 49 ¶¶ 93, 108, 112, 115, 117, 119), she has alleged the disclosure of Private Information (*see supra* Section III.B.1). However, that Plaintiff has alleged the disclosure of highly sensitive information does not negate the lack of allegations regarding an intrusion in this case. The case Plaintiff cites in support of this argument, *R.C. v. Walgreen Company*, focuses on disclosure under California law, which is notably distinct from a disclosure claim under Washington law. 733 F. Supp. 3d 876 (C.D. Cal. 2024). Further, the *Walgreen* court did not focus on the issue of whether plaintiffs had alleged an intrusion; it focused on whether the disclosure was highly offensive. *See id.* at 893–94. For these reasons, *Walgreen* is unpersuasive here.

Accordingly, as to Plaintiff’s claim for invasion of privacy, Defendant’s motion is GRANTED without leave to amend.

1 **4. Count III: Breach of Implied Contract**

2 Plaintiff brings an amended claim for breach of implied contract on behalf of herself and
3 the putative nationwide class. Dkt. No. 49 at 39. Defendant seeks dismissal, arguing that Plaintiff
4 “still fails to allege the existence of a valid contract, supported by mutual assent and
5 consideration.” Dkt. No. 54 at 19.

6 “To prevail on a breach of implied contract claim, a plaintiff must demonstrate that [an]
7 implied contract exists based on the acts of the parties involved and in light of the surrounding
8 circumstances.” *Leslie v. Fidelity Nat. Title Ins. Co.*, 598 F. Supp. 2d 1176, 1184 (W.D. Wash.
9 2009) (citing *Caughlan v. Int’l Longshoremen’s & Warehousemen’s Union*, 52 Wn.2d 656, 328
10 P.2d 707 (1958)). Washington recognizes two classes of implied contracts: those implied in fact,
11 and those implied in law. *Young v. Young*, 164 Wn.2d 477, 191 P.3d 1258 (2008) (citing
12 *Chandler v. Wash. Toll Bridge Auth.*, 17 Wn.2d 591, 137 P.2d 97 (1943)). Plaintiff alleges a
13 contract implied in fact. Dkt. No. 55 at 14.

14 The Court previously determined that the provision of user data alone to Defendant in
15 exchange for services was insufficient to establish an implied-in-fact contract. *See* Dkt. No. 32 at
16 23. Plaintiff argues that her breach-of-implied-contract claim should survive because she now
17 specifically alleges that she “has paid for and received medical treatment from Defendant on a
18 recurring basis since approximately 2006.” Dkt. No. 55 at 14 (quoting Dkt. No. 49 ¶ 43). Like in
19 other cases the Court acknowledged in its original Order, allegations that Plaintiff provided
20 money *and* confidential medical information to Defendant in exchange for services are sufficient
21 to establish the existence of an implied contract at the motion-to-dismiss stage. *See, e.g., Doe v.*
22 *Boone Health, Inc.*, No. C22-7646, 2023 WL 4996117, at *3 (Mo. Cir. Ct. July 20, 2023); *Doe v.*
23 *Regents of Univ. of Cal.*, 672 F. Supp. 3d 813, 821 (N.D. Cal. 2023); *MarinHealth Medical*
24 *Group, Inc.*, 2024 WL 217841, at *4.

1 Reading Plaintiff’s allegations in the light most favorable to Plaintiff, this case is similar
2 to *MarinHealth* in that it “arises in the context of *paid* healthcare services and is based on an
3 ongoing relationship between the parties.” *MarinHealth*, 2024 WL 217841, at *4 (emphasis in
4 original). But here, Plaintiff specifically alleges that she “paid for *and received* medical
5 treatment from Defendant.” Dkt. No. 49 ¶ 43. While she alleges that Defendant “encourage[d]
6 Plaintiff . . . to use its digital tools, including its Website” (Dkt. No. 49 ¶ 29), she makes no
7 factual allegations that Defendant premised the provision of its medical treatments upon use of
8 its Website, or that she made any payment to Defendant specifically for the use of its public
9 Website. To the contrary, any payments Plaintiff made to Defendant are specifically alleged to
10 have been solely for medical services, which she also alleges to have received. *Compare* Dkt.
11 No. 49 ¶ 43, with *Boone Health*, 2023 WL 4996117, at *3 (“Plaintiff further alleges that
12 Defendants solicited and received consideration from Plaintiff for this implicit promise,
13 including monies paid for medical services *and* confidential medical information”
14 (emphasis added)), and *Regents*, 672 F. Supp. 3d at 821 (“Plaintiff alleges that she and other
15 class members paid money *and* provided their User Data to UC Regents in exchange for services
16” (emphasis added)). Thus, Plaintiff cannot premise her implied-contract claim upon her
17 payments to Defendant that she alleges were solely for medical services.

18 Plaintiff also argues that Defendant’s Online Privacy Notice can also form the basis of an
19 implied contract. Dkt. No. 55 at 15. But as the Court previously noted, “while such policies may
20 form the *terms* of an implied contract, they do not alone serve as an enforceable contract without
21 a separate ‘meeting of the minds’ between the parties.” Dkt. No. 32 at 23 (quoting *Doe v.*
22 *Regents*, 672 F. Supp. 3d at 821). And Plaintiff fails to allege that Defendant promised to act
23 above and beyond its existing HIPAA mandates in its Online Privacy Notice. While the Court
24 has determined that the information Plaintiff alleges was shared discloses patient status and is

1 therefore protected under HIPAA (*see supra* Section III.B.1), she still must allege that Defendant
2 made a promise to protect that information beyond what it is required to do under HIPAA. *See*,
3 *e.g.*, *Griffey*, 562 F. Supp. 3d at 52. Plaintiff has thus failed to allege the existence of an implied
4 contract.

5 Accordingly, as to Plaintiff's claim for breach of implied contract, Defendant's motion is
6 GRANTED with leave to amend.

7 **5. Count IV: Unjust Enrichment**

8 Plaintiff brings an amended claim for unjust enrichment on behalf of herself and the
9 putative nationwide class. Dkt. No. 49 at 40. Defendant seeks dismissal, arguing that Plaintiff
10 has failed to plead either a concrete detriment or that the circumstances in this case make it
11 unjust for Defendant to retain any benefit conferred. Dkt. No. 54 at 20.

12 To state a claim for unjust enrichment, Plaintiff must show that: (1) Plaintiff conferred a
13 benefit upon Defendant, (2) at Plaintiff's expense, and (3) the circumstances make it unjust for
14 Defendant to retain the benefit without payment. *Young v. Young*, 164 Wn.2d 477, 484 (2008).

15 As the Court noted in its prior Order, "the provision of any PHI to Defendant would be
16 sufficient to confer a benefit." Dkt. No. 32 at 25. Because Plaintiff now has adequately alleged
17 the provision of her Private Information to Defendant (*see supra* Section III.C.1), Plaintiff has
18 alleged the conferral of a benefit upon Defendant for the purposes of her unjust-enrichment
19 claim. *See Boone Health*, 2023 WL 4996117, at *4 (finding that plaintiff had conferred a benefit
20 on defendants in the form of valuable and confidential medical information); *see also In re*
21 *Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 412–13 (E.D. Va. 2020)
22 (finding that benefit was conferred to Amazon where it "profited from its storage and retention
23 of Plaintiffs' PII").
24

1 Next, the Court turns to an assessment of whether the SAC alleges that the benefit
2 conferred was at Plaintiff's expense. The Court previously held that Plaintiff's general
3 contentions—void of any factual support that she “suffered from[] ‘(i) invasion of privacy,
4 (ii) lost time and opportunity costs associated with attempting to mitigate the actual
5 consequences of the Pixel, (iii) loss of benefit of the bargain, (iv) diminution of value of the
6 Private Information, (v) statutory damages, and (vi) the continued and ongoing risk to their
7 Private Information”—were insufficient to establish a concrete detriment. Dkt. No. 32 at 26. But
8 while Plaintiff now specifically identifies what private information she shared with Defendant
9 and contends was shared with third parties, the loss of privacy alone is insufficient to establish a
10 benefit conferred at Plaintiff's expense for purposes of an unjust-enrichment claim. “In
11 Washington, alleging a non-economic loss, such as a loss of privacy, is insufficient [to establish
12 an expense to plaintiff] because ‘Washington courts have not applied the doctrine
13 of unjust enrichment outside the context of an “expense” stemming from some tangible
14 economic loss to a plaintiff.’” *Vance v. Microsoft Corp.*, 525 F. Supp. 3d 1287, 1299 (W.D.
15 Wash. 2021) (quoting *Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116, 1130 (W.D. Wash.
16 2012))).

17 Accordingly, as to Plaintiff's claim for unjust enrichment, Defendant's motion is
18 GRANTED with leave to amend.

19 **6. Count V: Breach of Fiduciary Duty**

20 Plaintiff newly brings a claim for breach of fiduciary duty against Defendant on behalf of
21 herself and the putative nationwide class. Dkt. No. 49 at 41. Defendant moves to dismiss,
22 arguing that there is no precedent to recognize a duty of a healthcare provider in its capacity as a
23 website operator. Dkt. No. 54 at 23–24.

1 “A claim for breach of fiduciary duty requires a plaintiff to prove ‘(1) existence of a duty
2 owed, (2) breach of that duty, (3) resulting injury, and (4) that the claimed breach proximately
3 caused the injury.’” *Priv. Client Fiduciary Corp. v. Chopra*, No. C22-436, 2023 WL 2372917, at
4 *6 (W.D. Wash. Mar. 6, 2023) (quoting *Micro Enhancement Int’l, Inc. v. Coopers & Lybrand,*
5 *LLP*, 110 Wn. App. 412, 433–34, 40 P.3d 1206 (2002)).

6 While Washington courts do not appear to have addressed a breach-of-fiduciary-duty
7 claim against a healthcare provider for the disclosure of private information, other courts have
8 recognized that “[a] confidential and fiduciary duty may arise when a patient trusts the
9 [healthcare provider] defendant with their confidential health information,” as Plaintiff here has
10 done. *Allen v. Novant Health, Inc.*, No. C22-697, 2023 WL 5486240, at *5 (M.D.N.C. Aug. 24,
11 2023); *see also Doe v. Tenet Healthcare Corp.*, 731 F. Supp. 3d 142, 151 (D. Mass. 2024);
12 *Cooper v. Mount Sinai Health Sys., Inc.*, 742 F. Supp. 3d 369, 385 (S.D.N.Y. 2024). *But see In*
13 *re U.S. Vision Data Breach Litig.*, 732 F. Supp. 3d 369 (D.N.J. 2024) (finding no fiduciary
14 relationship between patient and retailer of optical products and services where patients did not
15 have direct relationship with retailer).

16 Plaintiff, a patient of Defendant, has stated a viable claim for breach of fiduciary duty
17 against her healthcare provider for disclosing her Private Information. *See In re Shields Health*
18 *Care Grp., Inc. Data Breach Litigation*, 721 F. Supp. 3d 152, 165 (D. Mass. 2024) (“Plaintiffs
19 have adequately pleaded that as their healthcare provider, Shields was their fiduciary.”). Plaintiff
20 alleges that Defendant regularly encouraged her to use its website to receive healthcare services.
21 Dkt. No. 49 ¶ 29. Plaintiff further alleges that she placed Defendant in a position of trust by
22 using its platform to communicate Private Information. *Id.* ¶ 225. She alleges that Defendant
23 breached that fiduciary duty by disclosing her PHI, and the Court has already determined that
24 Plaintiff has sufficiently alleged such a disclosure. *See supra* Section III.B.1.

1 Accordingly, as to Plaintiff's claim for breach of fiduciary duty, Defendant's motion is
2 DENIED.

3 **7. Count VI: Violation of the Electronic Communications Privacy Act**
4 **("ECPA")**

5 Plaintiff brings an amended claim for violations of ECPA on behalf of herself and the
6 putative nationwide class. Dkt. No. 49 at 43. Defendant seeks dismissal, arguing that Plaintiff
7 fails to allege any unlawful interception, that there is no civil liability for the alleged
8 "procurement" by Defendant, and that Plaintiff fails to allege the disclosure of any "contents."
9 Dkt. No. 54 at 25–28.

10 A claim under the ECPA "requires a showing that the defendant '(1) intentionally
11 (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to
12 intercept (3) the contents of (4) an electronic communication, (5) using a device.'" *See In re*
13 *Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 844 (N.D. Cal. 2017) (quoting *In re*
14 *Google Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 135 (3d Cir. 2015))

15 The Court previously dismissed Plaintiff's ECPA claim because Defendant did not
16 unlawfully intercept its own communications with Plaintiff, and because the tortious or criminal-
17 act exception did not apply. *See* Dkt. No. 32 at 28–30. Plaintiff contends that her amended claim
18 clearly alleges a criminal or tortious purpose for Defendant's interception, making the tortious or
19 criminal-act exception applicable. Dkt. No. 55 at 22–23.

20 As the Court stated in its prior Order, "[c]ourts within this Circuit have held 'that a
21 plaintiff must plead sufficient facts to support an inference that the offender intercepted the
22 communication for the purpose of a tortious or criminal act that is *independent* of the intentional
23 act of recording or interception itself.'" *B.K. v. Eisenhower Med. Ctr.*, 721 F. Supp. 3d 1056,
24 1065 (C.D. Cal. 2024) (emphasis in original) (citing *Pena v. GameStop*, 670 F. Supp. 3d 1112,

1 1119 (S.D. Cal. 2023)). Plaintiff argues that “Defendant’s conduct falls squarely within the
2 crime/tort exception because it intended to violate various tort and criminal laws through the
3 interception of Plaintiff’s communications, including HIPAA’s criminal prohibitions against
4 disclosing ‘individually identifiable health information’ without authorization.” Dkt. No. 55 at
5 22–23.

6 But as this Court previously determined, Plaintiff must allege a tortious or criminal use of
7 the acquired communications *separate* from their recording, interception, or transmission for the
8 tortious or criminal-act exception to apply. *See* Dkt. No. 32 at 30; *see also Pena*, 670 F. Supp. 3d
9 at 1119. Plaintiff’s amended pleadings still allege that the technologies installed by Defendant
10 contemporaneously transmit Plaintiff’s communications to third parties. Dkt. No. 49 ¶ 13. And
11 Plaintiff’s own argument demonstrates that the alleged tortious or criminal use of the acquired
12 communications is the disclosure itself. *See* Dkt. No. 55 at 22–23.

13 Plaintiff argues that other federal courts have found “substantially identical allegations
14 sufficient to trigger the crime-tort exception” and this Court should do the same. Dkt. No. 55 at
15 23. But none of the cases cited by Plaintiff evaluate the distinction between the interception and
16 transmission of data. *See Kurowski*, 2023 WL 8544084; *In re Grp. Health Plan Litig.*, 709 F.
17 Supp. 3d 707; *Kane v. Univ. of Rochester*, No. C23-6027, 2024 WL 1178340 (W.D.N.Y. Mar.
18 19, 2024); *Mekhail v. N. Mem’l Health Care*, 726 F. Supp.3d 916 (D. Minn. 2024); *In re Meta*
19 *Pixel Healthcare Litig.*, 647 F. Supp. 3d at 797; *B.K. v. Desert Care Network*, No. C23-5021,
20 2024 WL 1343305, at *6 (C.D. Cal. Feb. 1, 2024). In *Williams v. TMC Health*, a similar case
21 against a hospital system for data-sharing via the Facebook Pixel and similar tracking
22 technologies on its public website, the Court found that plaintiffs’ claim under the ECPA failed
23 because the crime-tort exception did not apply. No. C23-434, 2024 WL 4364150, at *4 (D. Ariz.
24 Sept. 30, 2024). The *Williams* court concluded that plaintiffs’ own allegations that “[d]efendant

1 used these technologies ‘to obtain valuable personal data about visitors to its Website, . . . to
 2 increase its own profits through sophisticated and targeted advertising[,] and to improve its
 3 website analytics’” pointed to “a non-criminal, non-tortious purpose” under the ECPA. *Id.*
 4 (internal citation omitted). Thus, the court determined that plaintiffs had failed to allege a
 5 criminal or tortious purpose for the transmission of data sufficient to trigger the crime-tort
 6 exception. *Id.* Plaintiff’s allegations here are similar; they point to a non-criminal, non-tortious
 7 purpose for Defendant’s use of the acquired communications. *See, e.g.*, Dkt. No. 49 ¶ 127.
 8 Consequently, the Court declines to depart from its previous analysis. Plaintiff still fails to plead
 9 a tortious or criminal use of the acquired communications, separate from their recording,
 10 interception, or transmission.⁶ *See generally* Dkt. No. 49.

11 Accordingly, as to Plaintiff’s ECPA claim, Defendant’s motion is GRANTED without leave
 12 to amend.

13 **8. Count VII: Violation of RCW §§ 7.70.010–.160**

14 Plaintiff newly brings a claim for violation of RCW §§ 7.70.010–.160 on behalf of
 15 herself and the putative nationwide class. Dkt. No. 49 at 49. Defendant seeks dismissal, arguing
 16 that this is not a case involving “health care” under the statute and that this is not a medical
 17 malpractice case. Dkt. No. 54 at 24.

18 A claim of medical negligence under RCW Chapter 7.70 “requires a showing of duty,
 19 breach, and proximate causation.” *Stevens v. Pierce County*, No. C22-5862, 2023 WL 5177915,
 20 at *6 (W.D. Wash. Aug. 11, 2023). Defendant argues that “[v]irtually all of the case law
 21 interpreting RCW § 7.70 *et seq.* concerns a health care provider or physician’s *actual*
 22 *malpractice*, not use of website analytics,” and that there is no duty of a healthcare provider in its

23
 24 ⁶ Because Plaintiff has still not alleged the first prong of an ECPA claim, the Court declines to address the Parties’ additional arguments with respect to Plaintiff’s ECPA claim.

1 capacity as a website operator. Dkt. No. 54 at 24 (emphasis in original). However, as Plaintiff
 2 notes, Washington courts recognize “a cause of action against physicians [under chapter 7.70]
 3 for unauthorized disclosure of privileged information.” *Berger v. Sonneland*, 144 Wn.2d 91, 106,
 4 26 P.3d 257 (2001) (citing *Loudon v. Mhyre*, 110 Wn.2d 675, 680, 756 P.2d 138 (1988)). While
 5 Defendant contends that “Overlake is not a ‘physician’ but rather a hospital/website operator
 6 here” (Dkt. No. 56 at 13), “healthcare provider” under RCW Chapter 7.70 “also includes
 7 nonhuman actors, such as a ‘hospital,’ ‘facility, or institution’ that employs a person providing
 8 health care.” *M.N. v. MultiCare Health Sys., Inc.*, 2 Wn.3d 655, 662, 541 P.3d 346 (2024).

9 However, Defendant also argues that this case does not involve “health care” under the
 10 statute because “it has nothing to do with the diagnosis, treatment, or care of a patient.” Dkt.
 11 No. 56 at 13; *see also MultiCare Health Sys.*, 2 Wn.3d at 662 (“However, for a plaintiff’s claim
 12 to fall under chapter 7.70 RCW, the injury must occur ‘as a result of health care.’”). “[H]ealth
 13 care’ under chapter 7.70 RCW is the process by which any healthcare provider uses the skills
 14 they have been taught to examine, diagnose, treat, or care for the plaintiff as their patient.”
 15 *MultiCare Health Sys.*, 2 Wn.3d at 662. The Washington Supreme Court has already determined
 16 that the negligent disclosure of confidential medical history may fall within the scope of chapter
 17 7.70. *See MultiCare Health Sys.*, 2 Wn.3d at 665; *Berger*, 144 Wn.2d at 95–96. Still, Defendant
 18 argues that *Berger* is distinguishable because it concerned “a physician’s disclosure of a patient’s
 19 confidential medical information ‘in his effort to discover more about Respondent’s use of pain
 20 medications so he could treat, diagnose, or care for her.’” Dkt. No. 57 at 13–14 (citing *Berger*,
 21 144 Wn.2d at 110). Plaintiff alleges that Defendant’s use of third-party trackers “allows
 22 Defendant to optimize the delivery of ads, measure cross-device conversations, create custom
 23 audiences, and decrease advertising and marketing costs.” Dkt. No. 49 ¶ 100. Plaintiff also
 24 alleges that “Defendant[] benefitted from this unlawful practice with more efficient marketing

1 that resulted in savings, as well as the acquisition of new patients that added value to the
2 Hospital's revenue and growth." *Id.* ¶ 38. But Plaintiff does *not* allege that Defendant utilized the
3 disclosure of information in order to treat, diagnose, or care for Plaintiff as its patient.

4 Because Plaintiff does not allege that her injury occurred as a result of "health care" as
5 defined under RCW §§ 7.70.010–.160, she has not alleged a claim for medical malpractice.

6 Accordingly, as to Plaintiff's claim under RCW Chapter 7.70, Defendant's motion is
7 GRANTED with leave to amend.

8 **9. Count VIII: Violation of the Washington Consumer Protection Act ("CPA")**

9 Plaintiff brings an amended claim for violation of the CPA. Dkt. No. 49 at 50. Defendant
10 seeks dismissal, arguing that Plaintiff has failed to allege a cognizable injury under the CPA.
11 Dkt. No. 54 at 29.

12 The CPA provides that "[u]nfair methods of competition and unfair or deceptive acts or
13 practices in the conduct of any trade or commerce are hereby declared unlawful." RCW
14 19.86.020. "To prevail in a private CPA claim, the plaintiff must prove (1) an unfair or deceptive
15 act or practice, (2) occurring in trade or commerce, (3) affecting the public interest, (4) injury to
16 a person's business or property, and (5) causation." *Panag v. Farmers Ins. Co. of Wash.*, 166
17 Wn.2d 27, 37, 204 P.3d 885 (2009) (citing *Hangman Ridge Stables, Inc. v. Safeco Title Ins. Co.*,
18 105 Wn.2d 778, 784, 719 P.2d 531 (1986)). Either an unfair or a deceptive act can be the basis
19 for a CPA claim. *Klem v. Wash. Mut. Bank*, 176 Wn.2d 771, 787, 295 P.3d 1179 (2013).

20 The Court previously determined that while Plaintiff did not need to allege she was an
21 active participant in the market for private information in order to allege injury, she had not
22 made sufficient factual allegations regarding her injury. *See* Dkt. No. 32 at 33. Plaintiff argues
23 that she is injured because she "had a property right taken from her; she cannot sell her
24 information to Facebook now." Dkt. No 55 at 27. But this argument is unpersuasive, given that

1 Plaintiff makes no allegations in the SAC regarding the market for sale of private information to
2 Facebook or that she ever attempted to or planned to sell her private information to Facebook.

3 However, as the Court previously noted, in other data-privacy cases under the CPA,
4 plaintiffs have provided substantial allegations regarding the loss of economic value of their
5 information *and* the time or money spent remedying the disclosure of the private information.
6 *See Guy v. Convergent Outsourcing, Inc.*, No. C22-1558, 2023 WL 4637318, at *1 (W.D. Wash.
7 July 20, 2023). Plaintiff does include factual allegations detailing the value of her Personal
8 Information, including her protected health information, but she does not provide sufficient
9 allegations regarding any time or money spent to remedy the disclosure of her Private
10 Information, and she cites to no caselaw indicating that loss of value alone is sufficient to
11 establish a harm for purposes of a Washington CPA claim. *See* Dkt. No. 49 ¶¶ 122–28.

12 Accordingly, as to Plaintiff's CPA claim, Defendant's motion is GRANTED with leave to
13 amend.

14 IV. CONCLUSION

15 For the reasons stated, the Court ORDERS as follows:

- 16 1. Defendant's motion to dismiss (Dkt. No. 54) is GRANTED IN PART and DENIED IN
17 PART . Plaintiff's claims for negligence, breach of implied contract, unjust
18 enrichment, violation of RCW §§ 7.70.010–.160, and violation of the Washington
19 CPA are DISMISSED with leave to amend. The Court will GRANT Plaintiff one final
20 opportunity to amend her complaint. Should she choose to do so, the final
21 amended complaint SHALL be filed by **March 25, 2025**.
- 22 2. Plaintiff's claims for invasion of privacy and violation of ECPA are DISMISSED
23 without leave to amend.

24 Dated this 4th day of March 2025.



Tana Lin
United States District Judge